CaptureBites
DORA Compliance Statement

Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA)

CaptureBites BV issues this statement to inform customers, in particular financial entities within the scope of Regulation (EU) 2022/2554 ("DORA"), of the measures CaptureBites has in place as an ICT third-party service provider. This document is intended as a general reference and can be supplemented with entity-specific contractual annexes, service level agreements or due-diligence questionnaires upon request.

About CaptureBites

CaptureBites BV is a software company established in 2014 and based in Antwerp, Belgium. Our focus is intelligent automation for document processing and data capture, turning scanned and digital documents into structured, usable data.

Our flagship product is MetaServer, an IDP (Intelligent Document Processing) platform that handles Email, PDF, TIF, JPG and other file types from end to end. MetaServer separates document sets, extracts and formats key data, validates results against database lookups and business rules and converts files to searchable PDF. The result flows straight into the system of your choice. Send a document to MetaServer, and it triggers the solution to run every step automatically, based on rules you configure with no coding required.

CaptureBites also provides connectors to add functionality to the following Tungsten Automation scan software:
- Tungsten Express (previously known as Kofax Express)
- Tungsten Capture (previously known as Kofax Capture)
- Tungsten TotalAgility (previously known as Kofax TotalAgility)

CaptureBites focuses on development. Sales and support run through our network of local partners and distributors.

DORA & CaptureBites

CaptureBites acts as an ICT third-party service provider within the meaning of DORA when its software or services support the operations of a financial entity, whether supplied directly or via an implementation partner or reseller.

CaptureBites recognizes that financial-entity customers remain responsible for their own DORA compliance and that CaptureBites' role is to support that compliance through the measures described in this document.

CaptureBites
DORA Compliance Statement

Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA)

MetaServer

ICT Risk Management

CaptureBites maintains an ICT risk management approach covering secure development practices, access control and vulnerability management for MetaServer. This includes restricting source code access to authorized individuals under the principle of least privilege and logging all source code changes. Further detail on secrets handling and source code management is provided in this section's "Data & Security Management - Source Code Management".

Data & Security Management

The following describes, at a technical level, how MetaServer handles authentication, data in transit, and data at rest within a customer's on-premise environment.

Authentication and Authorization

Users authenticate to their own workstation using their organization's existing Active Directory or Entra ID corporate account; no separate login is required within the MetaServer client itself. Access to documents and batches can be restricted at Active Directory / Entra ID user group or individual user level, so that only the users for whom a document is reserved are able to access it.

Reserving documents is optional: batches can instead be left unreserved and made available to any operator working from the operator client, in which case there is no link to the customer's Active Directory / Entra ID.

Data in Transit

Importers and clients (such as Admin or Operator) communicate with the MetaServer server using database protocols for lookups and updates, HTTPS for licensing and SMB for data traffic between clients and the server. Database lookups containing metadata are exchanged using the relevant database manufacturer's protocol, for example standard SQL commands when the database server is Microsoft SQL Server.

Documents and their extracted metadata are transferred to and from the file system using the SMB (TCP 445) protocol. License activation uses a secure (SSL) connection; no document content or metadata is transmitted or accessed during this process. Activation occurs only once at installation and again only if new modules are added or the license needs to be refreshed.

Data at Rest

MetaServer is designed around an **ephemeral pipeline architecture**.

Images and metadata are only temporarily stored in the data folder on the MetaServer server and are automatically deleted once a document has finished processing, typically once it has been exported to its final destination.

While present, images and extracted metadata are secured through Windows file system permissions. Passwords used for external systems or application-specific accounts (such as email, FTP, or database accounts) are always stored using an encryption algorithm.

Secrets Management

Secrets, such as service account passwords, API keys, and cipher keys are not included in MetaServer's source code or scripts. Access to secret information is restricted to administrators, who manage it exclusively through dedicated setup dialogs in the MetaServer Admin client, in line with the principle of least privilege. Administrators can configure different secrets across the production environment and other environments (e.g. staging) and are able to renew secrets periodically. During entry, passwords are obfuscated and are never displayed in clear text.

Source Code Management

MetaServer's source code is accessible only to authorized individuals, with access managed following the principle of least privilege, and is classified as confidential by default.

All of CaptureBites' source code, build configuration manifests, and integration scripts are hosted within secured, private Git version control repositories. Public access is blocked, and indexing by external web search engines or unauthorized third parties is restricted.

Third-Party and Open-Source Components

MetaServer does not incorporate third-party open-source components, which removes a class of supply-chain and open-source vulnerability exposure that would otherwise need to be separately inventoried and managed.

Information Security

Data passes through the application for processing purposes only and is not hosted, retained or stored by CaptureBites. CaptureBites applies measures to protect the confidentiality of customer data during processing through MetaServer, including:

- *Ongoing monitoring and review of infrastructure and applications to manage security risks and vulnerabilities*
- *On-premise deployment within the customer's own infrastructure and under the customer's control*

Connectors for Tungsten Automation scan software

ICT Risk Management

CaptureBites maintains an ICT risk management approach covering secure development practices, access control and vulnerability management for the export connectors we provide for the previously mentioned Tungsten Automation scan software. This includes restricting source code access to authorized individuals under the principle of least privilege and logging all source code changes. Further detail on secrets handling and source code management is provided in this section's "Data & Security Management - Source Code Management".

Data & Security Management

The following describes, at a technical level, how our connectors for Tungsten Automation scan software handle authentication, data in transit, and data at rest within a customer's on-premise environment.

Authentication and Authorization

Users authenticate to their own workstation using their organization's existing Active Directory or Entra ID corporate account; no separate login is required within the export connector itself.

Data in Transit

CaptureBites connectors act as a **secure transit bridge** between the host document capture environment (Tungsten Express, Tungsten Capture and Tungsten TotalAgility) and destination repositories, such as Microsoft SharePoint, Box, Alfresco, OpenText, SAP, Xerox DocuShare, IBMCMOD, relational databases, or SFTP endpoints.

All network data flows initiated by CaptureBites connectors enforce end-to-end cryptographic protection, protocol integrity, and strict boundary controls.

It also can export to a folder structure on the customer's local system, by which it complies to the customer's security measures.

Data at Rest

CaptureBites connectors are designed around an **ephemeral pipeline architecture**, functioning strictly as stateless transformation and delivery engines within the host document processing runtime (Tungsten Capture, Tungsten TotalAgility, and Tungsten Express). Long-term retention of data is deliberately excluded from the connector footprint, minimizing storage-level attack surfaces and eliminating unauthorized persistence.

Secrets Management

CaptureBites connectors interact with diverse enterprise systems, requiring secure handling of authentication secrets such as OAuth 2.0 client secrets, refresh tokens, service account credentials, database connection strings, and private API keys. CaptureBites enforces a strict "Zero Cleartext" secrets policy to prevent credential harvesting, configuration file inspection, and unauthorized lateral movement within banking infrastructure.

Source Code Management

The connectors' source code is accessible only to authorized individuals, with access managed following the principle of least privilege, and is classified as confidential by default.

All of CaptureBites' source code, build configuration manifests, and integration scripts are hosted within secured, private Git version control repositories. Public access is blocked, and indexing by external web search engines or unauthorized third parties is restricted.

Third-Party and Open-Source Components

Our connectors for Tungsten Automation scan software do not incorporate third-party open-source components, which removes a class of supply-chain and open-source vulnerability exposure that would otherwise need to be separately inventoried and managed.

Information Security

Data passes through the connectors for processing purposes only and is not hosted, retained or stored by CaptureBites. CaptureBites applies measures to protect the confidentiality of customer data during processing through the connectors, including:

- *Ongoing monitoring and review of infrastructure and applications to manage security risks and vulnerabilities*
- *On-premise deployment within the customer's own infrastructure and under the customer's control*

CaptureBites
DORA Compliance Statement

Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA)

General

Incident Management

CaptureBites maintains procedures to identify and respond to ICT-related incidents. Where an incident materially affects a customer's use of either a connector for Tungsten Automation scan software or MetaServer, CaptureBites will notify the affected customer without undue delay. Support case handling, severity classification, and associated response times are further described in CaptureBites' Software Upgrade Assurance (SUA), available at https://www.capturebites.com/SUA/.

Business Continuity

CaptureBites maintains business continuity arrangements intended to limit disruption to Tungsten Automation scan software caused by our connectors and MetaServer services.

Cooperation with authorities

CaptureBites is committed to cooperating with competent supervisory and regulatory authorities and providing information reasonably requested in connection with a customer's regulatory obligations.

Transition support

In the event a customer relationship or service ends, CaptureBites will provide reasonable transition assistance to help the customer maintain operational continuity in line with its own exit-management obligations under DORA.

Termination rights

The customer may terminate this agreement, any associated software license, or support/maintenance contract immediately upon written notice, without penalty or liability for early termination, upon the occurrence of any of the following events:

- Significant Breach: A material or persistent breach by CaptureBites of applicable laws, regulations, security standards, or contractual terms (including sustained failure to meet agreed SLA thresholds for critical software patches, connector compatibility fixes, or zero-day vulnerability mitigations).
- Impairment of Performance: Circumstances identified through the customer's ongoing monitoring of ICT third-party risk capable of altering or degrading the performance of MetaServer or CaptureBites connectors for Tungsten Automation scan software, including:
    - Material changes in CaptureBites' ownership, control, corporate structure, or financial standing;
    - Inability or refusal by CaptureBites to maintain ongoing API and runtime compatibility between CaptureBites Connectors and supported Tungsten Automation scan software updates;
    - Unannounced discontinuation of maintenance for key functional components.
- Weaknesses in ICT Risk Management: Evidenced material weaknesses or systemic vulnerabilities in CaptureBites' security practices, software development lifecycle (SDLC), or patch management that jeopardize the availability, authenticity, integrity, or confidentiality of document data processed via MetaServer or CaptureBites connectors for Tungsten Automation scan software.
- Supervisory or Resolution Authority Order: A formal instruction, finding, or order from a competent supervisory authority or resolution authority (e.g., ECB, EBA, EIOPA, or national competent authority) stating that:
    - The authority can no longer effectively supervise the customer due to the terms of the arrangement.
    - The customer must terminate or replace the software to ensure digital operational resilience.

- Insolvency and Discontinuation: CaptureBites enters liquidation, administration, bankruptcy, or discontinues commercial operations.

Since MetaServer licenses are perpetual, the license itself will not be terminated / become invalid. As soon as the customer explicitly requests to terminate the use of their license, any maintenance contracts will cease being actively renewed.

The same applies for CaptureBites connectors for Tungsten Express, Tungsten Capture and Tungsten TotalAgility.

Contact

For questions regarding this statement, DORA-related due diligence or to request supplementary documentation, please contact info@capturebites.com.

On behalf of CaptureBites BV

JD Moons
Chief Executive Officer
CaptureBites BV

CaptureBites BV — Antwerp, Belgium
This statement is provided for informational purposes and does not itself constitute a binding contractual commitment; specific obligations are set out in the applicable customer agreement and CaptureBites' End User License Agreement (EULA), available at https://www.capturebites.com/eula/.